**IN THE UNITED STATES DISTRICT COURT**
**FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| IN THE MATTER OF THE SEARCH OF THE PROPERTY LOCATED AT: | ) | 1:23-mc-00384 |
| **27945 GREAT COVE ROAD FORT LITTLETON, PA 17223** | ) | |

# AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Justin Kurtz, being first duly sworn, hereby depose and state:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to State College, PA and have been so employed since April 2017. Additionally, I have served as an instructor at the HSI Academy located at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA. I am responsible for investigations involving the production, importation, advertising, receipt, and distribution of Child Sexual Abuse Material which occur in the Middle District of Pennsylvania. I have participated in multiple Child Sexual Abuse Material (CSAM) investigations. I have received training in the area of Child Sexual Abuse Material and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and Child Sexual Abuse Material crimes.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits and evidence specified in Attachment B herein for the premises located at 27945 Great Cove Rd, Fort Littleton, PA 17223 as further identified in Attachment A and referred to hereinafter from time to time as the "SUBJECT PREMISES."

4. The information contained within this affidavit is based on my training and experience, as well as information I have developed, and information relayed to me by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable

cause to believe that instrumentalities, fruits and evidence of violations of 18 U.S.C. §§ 2252 and 2252A, are located at 27945 Great Cove Rd, Fort Littleton, PA 17223.

5. The application for a search warrant, which this affidavit is offered in support thereof, is being applied for to seize instrumentalities, fruits and evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess Child Sexual Abuse Material and access with intent to view Child Sexual Abuse Material, and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute Child Sexual Abuse Material.

6. In summary, this affidavit sets forth facts establishing probable cause to believe that within the SUBJECT PREMISES there are instrumentalities, fruits and evidence of a subject who received, distributed, and/or possessed via the Internet, images depicting minors engaging in sexually explicit conduct.

## RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

8. 18 U.S.C. §§ 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (Child Sexual Abuse Material) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (Child Sexual Abuse Material).

## DEFINITIONS

The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

f. The term "GUID", as used herein refers to the Globally Unique Identifier (GUID) identification number that may be issued by the Peer-to-Peer (P2P) software to computers offering to share files on the P2P network. A GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

g. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

h. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but

not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices, portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

## BACKGROUND ON PEER-TO-PEER NETWORKS

9. Your affiant knows through training and experience one of the fast-growing areas that facilitates and is used by Child Sexual Abuse Material collectors and traders is peer-to-peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. The P2P Networks, such as such as FastTrack, eDonkey, BitTorrent , Ares and the Gnutella have become ideal for traders to openly exchange collections and share those collections. The P2P network has provided a way for traders to have what they feel is an open and anonymous distribution and trading network. This network enables trading on a world-wide basis and with upload and download speeds as if the trader was next door.

10. Your affiant knows that computers on these networks have software installed on them that facilitate the trading of images. The software, when installed, allows the user to search for pictures, movies and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, eDonkey, BearShare, Frostwire, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients.

11. P2P file sharing networks are frequently used to trade digital files of Child Sexual Abuse Material. These files include both image and movie files. P2P file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files.

12. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

13. To access the P2P networks, a user first must purposely seek out P2P software for sharing on the internet and then obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide P2P network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network and on the user's bandwidth and firewall settings. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network.

14. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, information about the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then purposefully selects file(s) which he/she wants to download. There is no accidental download process. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event.

15. Thus, a person interested in sharing Child Sexual Abuse Material with others in the P2P network, need only place those files in his/her "shared" folder(s) or leave the files they

download in the shared folder. Those Child Sexual Abuse Material files are then available to all users of the P2P network for download regardless of their physical location.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time thus speeding up the rate at which a single file is downloaded. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The user's computer then reassembles those parts into the single file. This reduces the time it takes to download the file. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular Internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

17. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to forcefully send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload Child Sexual Abuse Material files to another user's computer without his/her computer's active participation.

18. The investigation of peer-to-peer (P2P) file sharing networks is a cooperative effort of law enforcement agencies around the country. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing Child Sexual Abuse Material, some of which were also involved in the active sexual exploitation of actual child victims.

## BACKGROUND ON GNUTELLA NETWORK

19. Your affiant knows from experience that the Gnutella P2P network client software can only succeed in reassembling the movie from different parts if the parts all come from the exact same movie. In order to accomplish this, the Gnutella network has a built-in functionality to insure precise file matching. Precise file matching is done through the use of SHA-1 digital signatures. The method used by the Gnutella P2P network involves a file

encryption method called Secure Hash Algorithm version 1, or more commonly known as SHA-1. The National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), developed SHA-1. It has been accepted and adopted as the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS) by the United States of America as a Federal Information processing Standard. A SHA-1 value can be likened (in layman terms) to DNA but it is statistically more accurate than DNA comparison. It is in essence, a mathematical fingerprint of a computer file that will remain the same for an unchanged file no matter where the file is found or on which computer the file is located.

20. Your affiant has learned that digital files can be processed and have done processing of files during testing by this SHA-1 process, resulting in a digital signature. By comparing these digital signatures, I can conclude that two files are identical with a precision that greatly exceeds the statistics of DNA testing and matching on humans and can know for a certainty without actually opening the file what it is based on its digital signature. Accordingly, that kind of certainty can be used to state for probable cause that a file with a SHA1 or digital signature that matches a digital signature of known Child Sexual Abuse Material that is found on a computer during an undercover transaction probably has that file and is probably in possession of Child Sexual Abuse Material (the certainty is much greater in reality than probable cause).

21. Your affiant has been able to validate by working similar cases and through working and training with other law enforcement officers, the fact that users attempting to trade files on the Gnutella file-sharing network could place files from their local computer in a shared folder. If that same user then starts the Gnutella software, that local computer could then calculate the SHA-1 signature for each file in the shared folder and provide that information to other users wishing to trade files. Your affiant has learned that the Gnutella P2P network software clients that connect and share files on the network calculate the SHA-1 value of files in the user's shared folder upon startup of the software. The Gnutella Client Software makes those values available on the network for comparison through the Ultra-peers so that multiple persons sharing one movie or file can deliver different pieces of that movie or file to the local software and the local software can ensure a complete and exact copy can be made from the parts.

22. Your affiant knows that when a user connects to the Gnutella Network those connections are initially made to Ultrapeers. Ultrapeers are the backbone of the Gnutella network. An Ultrapeer handles most of the searching on the Gnutella traffic. Users make

connections, upload information about the listing of their shared files and associated SHA-1 values of those files, and keep active open connections to those ultra-peers. When a request for a search goes out, the search goes through the ultra-peers. When a file is found and a request for that file is made the information about the file and the file then comes directly from the IP address that has the file because the ultra-peers only have the file listing type information and not the actual file. As a result there are many open connections to Ultrapeers during a peer-to-peer session. Ultrapeers do not have the actual files themselves but only serve as indexing pointers so that the requester can then direct his request for the actual file from the IP address that has the file.

23. Your affiant knows and has been able to confirm from use of the software and from downloads of files containing the same SHA-1 values that files received from different locations with identical SHA-1 values contain the same content. Each of the files may be named differently but contain the exact same file and content as long as the SHA-1 values were identical for each file.

24. Your affiant knows as previously stated that entering search query terms in the P2P software can result in a list of file names and their associated SHA-1 values that investigators could then choose from for download. By using this type of search, investigators can compare the offered SHA-1 values with known SHA-1 values associated with movie or image files known by the investigator or suspected by other investigators to be Child Sexual Abuse Material. Once a file with a SHA-1 value matching the SHA-1 value of a known or suspected Child Sexual Abuse Material file is located, the investigator can use the client software to obtain a list of specific IP address where computers are offering that same file. Those computers are called hosts and are offering a file that contains the identical Child Sexual Abuse Material file and are participating in the trade of known images that match known SHA-1 values of Child Sexual Abuse Material. This feature allows investigators to conduct undercover operations that involve images known or suspected to be Child Sexual Abuse Material and often involve identified child victims. In summary, this feature allows the investigator to identify the IP address of a computer that has connected to the P2P network and contains a file in the shared folder with a SHA-1 value associated with known or suspected Child Sexual Abuse Material at the time the computer was connected to the Gnutella P2P network.

25. Your affiant knows through training and experience that by examining the list of IP addresses reported by the client software to be sharing a particular file with a particular digital signature, you affiant could locate computers that are reported to be participating in distribution of CSAM. By doing a comparison of the SHA-1 values associated with the files being shared, your affiant can conclude that a computer, originating from an IP address known or believed to be in a certain area, has Gnutella P2P network client, or compatible, software installed on it and that the computer contains specific, known or suspected images of Child Sexual Abuse Material based on the SHA-1 values of the files on the computer. Those specific computers freely give me that information when asked as part of the inherent nature of the "file sharing" P2P network.

26. Your affiant knows through training and experience, that various P2P client software programs allow a user to interface with other users of the system. The client software allows a user of the Gnutella P2P network to search for files being voluntarily and openly shared on the network by other users, and that those files were automatically calculated with their SHA-1 values as a reference and comparison for the Gnutella Network. The various software programs allow the user to ask for a specific file listing of the contents of another user's shared files at a specified IP address on the network, or those files that a user elects to make public and available for other Gnutella Network users to download.

27. Your affiant has received training and has used the features built into the Gnutella P2P Client software programs to request a file listing of "shared files" from various computers during undercover P2P operations. The command used is commonly called a "browse." This command allows the computer host (a host is a term used to describe a computer connected to the Internet) making the request to "browse" or look through a listing of files by name, file type, quality and SHA-1 values that the user on the other end has specifically placed or downloaded into a specific folder for sharing with others on the P2P Network. A "browse" command is available to any and all users on the Gnutella Network. Users can share or have files in their shared folder available for searches and downloads on the Gnutella Network. Users can also disallow "browsing" of their shared files. Anyone who routinely uses and downloads files would know they are downloading from other users who have allowed file sharing on their computer as that is the whole concept and reason for installing a P2P client of software. Conversely, they would also know that certain files on their computer are available for download unless they intentionally change the configuration of the client software to disallow those downloads and

browsing commands from others on the network. Your affiant knows that when he uses the "browse" command, he is not going onto or into a computer and looking at files but merely making a publicly available request for that computer to send him the file list. When your affiant looks at that list, it is because the computer on the other end has freely and voluntarily sent it to your affiant and they have set up their computer with software that allows him or anyone on the network to make that open and public request.

28. Various law enforcement agencies use Gnutella client software to access the Gnutella Network and work undercover operations to identify IP addresses that share Child Sexual Abuse Material. Specifically, the software allows agents to display the SHA-1 values in the file listings returned in both the "browse" functions and the "file query" functions on the Gnutella Network. This same process can be used by anyone accessing the P2P network.

29. Your affiant knows that certain versions of the Gnutella software such as Shareaza are configured to access both the Gnutella network and the eDonkey Network. The eDonkey Network works similar but different to the Gnutella Network.

## BACKGROUND ON CHILD PROTECTIVE SYSTEM (CPS)

30. An investigation was conducted using the Child Protection System ("CPS") suite of tools. CPS suite of tools is a user-friendly system, harnessing the power and abilities of thousands of investigators working together in keeping and logging information through law enforcement servers, which are located in Boca Raton, Florida and owned by the Office of the State Attorney, 15th Judicial Circuit. CPS was created by, at the direction of, and remains maintained by law enforcement. CPS is a law-enforcement maintained database utilized by federal, state and local law enforcement agencies in child exploitation investigations worldwide. CPS maintains a log of IP addresses that have been previously involved in the possession and distribution of Child Sexual Abuse Material. Files are automatically compared to a known set of hash values as contained in the database that evidence Child Sexual Abuse Material from previous investigations by other law enforcement officers.

31. The data acquired from automated tools and undercover operations, including hash value, IP address offering to participate in distribution of a file, name of the file, date and time it was identified by CPS provided from the suspect computer, are all compiled into a user-friendly interface. HSI agents queried CPS for a particular geographic region or jurisdiction – in

this case, central Pennsylvania. Upon selecting an IP address to investigate, the information available from the servers historically about that IP address is generated and sent by CPS for the investigating agent to review.

32. In and through training and the registered use of CPS Suite of tools, Child Rescue Coalition has made available to Law Enforcement various scanners programed for capturing data about IP addresses offering to participate in the distribution of Child Sexual Abuse Material. Those tools are made based on the programming protocols for the P2P programs they access and do not hack or otherwise access computers that the normal P2P programs could not access. This suite of scanning tools made based on normal P2P programs are modified for law enforcement investigations to function within the CPS suite of tools, discussed above and record it's findings into that database. They simply record the offerings based on IP addresses and known or suspected offerings of Child Sexual Abuse Material. They read the publicly available information from computers that are identified as offering child sexual abuse images for distribution. This software reads these reported offers to participate in the sharing of Child Sexual Abuse Material and reports the time, date, SHA1 value GUID number of the software, and filename for each computer in a consistent and reliable manner to the undercover servers housed in Florida.

33. Some of the tools are as follows: Nordic Mule for the eDonkey Network, eCrawler and eScanner for the eDonkey Network, Peer Spectre, Limescanner, and Limecrawler for the Gnutella Network, G2 Scanner and G2 Crawler for the Shareaza only Gnutella-2 Network and ARES Crawler for the ARES Network.

34. The software is distributed and run by thousands of investigators whose software then contributes to a global database. HSI agents have access to those automated logs and can check and see who in and around this jurisdiction (Middle District of Pennsylvania) is participating in and offering Child Sexual Abuse Material for distribution on the P2P networks.

35. All the automated processes capture and populate date in what is called the CPS system that your affiant as an investigator has access to. The data acquired from automated tools and undercover operations, including hash value, IP address offering to participate in distribution of a file, name of the file, date and time it was identified by CPS provided from the suspect computer, are all compiled into a user-friendly password protected law enforcement web-based interface. HSI agents have access to those automated logs and can check and see who in and

around this jurisdiction (Middle District of Pennsylvania) is participating in and offering Child Sexual Abuse Material for distribution on the P2P networks.

36. The data about the IP address in this warrant comes from the scanning tools listed above. In the case at hand, your affiant queried CPS for a particular geographic region or jurisdiction. Upon selecting an IP address to investigate, the information available from the servers historically about that IP address is generated and sent by CPS for the investigating officer to review.

## BACKGROUND ON SHAREAZALE

37. Your affiant knows from training and experience this software is a designed by and for law enforcement and only available to law enforcement officer who have attended the appropriate training. ShareazaLE is designed to connect directly to one IP address and browse and/or download from one specific peer at a time blocking any swarming from other IP addresses. ShareazaLE is a peer-to-peer file-sharing client similar to other file -sharing clients (like LimeWire or Bearshare) on the Gnutella network which are free and available to the public. Shareaza specifically connects to both the Gnutella and eDonkey networks.

38. Using source code from a free and open source code peer-to-peer client (Shareaza), ShareazaLE was modified for law enforcement to meet the stringent investigative requirements of these cases. For example, ShareazaLE will only download files from a single source – the target IP, while the public version will download from many sources. ShareazaLE thus takes much longer to download files because of the single source limitation. ShareazaLE uses only publicly available P2P options, which follow the programming language (protocols) set forth in the public P2P protocol standards. No functionality outside of the publicly available protocols is added, thus eliminating any potential private intrusion on the suspect IP's computer or files. ShareazaLE uses the same code and language that is available to any and all software developers.

39. Upon locating an IP address on the peer-to-peer networks that is evidencing hash values of known images/videos of Child Sexual Abuse Material, the IP address is launched into the Undercover Investigative Software. An automated function of ShareazaLE will attempt to connect to the IP address when it is observed being "on-line" and [send a request to] browse (i.e. look at and log the information about shared files being transmitted and/or shown by that IP)

and/or download a file from the shared folder of the computer utilizing that IP address. If the connection is not made to either browse or download, ShareazaLE automatically continues to attempt to make a connection with the IP address.

40. If a connection is made with the suspect IP address, ShareazaLE will log the connection. It will also log the browse and/or download in the "logs" – the activity associated to IP activity. Files are then downloaded directly into an HSI computer [and segregated from any other evidence]. Prior to beginning an investigation ShareazaLE, your affiant specifically creates a folder structure on the hard drive of his own computer instructing ShareazaLE to the file path of where to store files that are downloaded and logs that are created. Both the downloaded files themselves as well as logs will be reported in the appropriate folders created for the targeted peer IP address by your affiant. The logs identify that a known hash value of Child Sexual Abuse Material has been located, that the download transfer started, that the transfer is in fact processing, and that the transfer of the file is complete. The length of time the download process takes depends on the size of the file and speed of the internet/computer of both the law enforcement computer, and the target IP's computer.

41. When a file has successfully completed the download process ShareazaLE notifies law enforcement. The software, being based on peer-2-peer program design, ensures that files are obtained directly from the target IP address – assuring a single-source download so that any downloaded file comes directly from the suspect IP address.

## BACKGROUND REGARDING SEIZURE OF COMPUTERS

42. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following.

43. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on

the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

44. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

45. In order to fully retrieve data from a computer system, the analyst needs all data storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

46. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone.

Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

## BACKGROUND REGARDING THE INTERNET/COMPUTERS AND CHILD SEXUAL ABUSE MATERIAL

47. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since 1997. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

48. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

49. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce Child Sexual Abuse Material easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the

method of distribution and receipt of Child Sexual Abuse Material. Child Sexual Abuse Material can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

50. The computer's capability to store images in digital form makes it an ideal repository for Child Sexual Abuse Material. A floppy or compact disk can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

51. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

52. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file

or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

## DETAILS OF INVESTIGATION

53. As part of undercover investigations, law enforcement agents around the country have devised a number of pro-active investigative techniques aimed at identifying and investigating individuals involved in the sexual exploitation of minors through the production, distribution, receipt and possession of Child Sexual Abuse Material (CSAM). One such technique is the use of P2P file-sharing software, to include the sharing of CSAM on ShareazaLE though the Gnutella and Edonkey networks. More specifically, IP address 174.54.12.128, which is an IP address identified as the target IP address for this investigation.

54. Historically, this target IP address (174.54.12.128) has been observed in CPS between the dates April 30, 2020 and April 14, 2023 responding to search requests for known or suspected CSAM. This IP address has responded over 29,700 times and has responded approximately 4,000 that it had 100% of the file. It has been seen responding on the network with known or suspected CSAM 9,804 times. During the times this IP has responded, the target computer said that it had 100% of the known or suspected CSAM files 2,397 times.

55. Your affiant served a DHS summons on Comcast Cable Communications, LLC for the IP address 174.54.12.128 on October 3, 2022. As result of the summons, Charter Communications, Inc provided the following account information:

| | |
|---|---|
| Name: | Jeremy MILLER |
| SSN: | 210-68-3967 |
| Address: | 27945 Great Cove Road |
| | Fort Littlton, PA 17223 |

Phone: (814) 641-1201

Account #: 8993111380008109

Service Start: 8/31/2019

56. According to Pennsylvania State Police, Jeremy MILLER was the perpetrator of a possible sexual assault on a minor child, approximately three years of age at the time of the assault, on or about June 23, 2015 in Saint Thomas, PA. Investigative reports revealed that the Pennsylvania State Police were unable to locate MILLER to speak with him regarding the incident and that a forensic interview with the victim was inconclusive.

57. According to law enforcement databases and open-source records, Jeremy Russel Miller with a date of birth of May 13, 1988 resides at 27945 Great Cove Rd, Fort Littleton, PA 17223 (SUBJECT PREMISES).

**58.** On November 29, 2022 your affiant observed the residence located at the SUBJECT PREMISES. The residence is a manufactured, single-family home, blue in color, with white trim and blue shutters. Attached to the front of the residence is a porch with a metal roof with multiple pieces of furniture and a riding lawn mower parked underneath. Attached to the corner of the roof of the porch was a green sign with numbers reading "27945." Located directly in front of the residence is a mailbox which, at the time of surveillance, was observed to have mail inside it and a green sign with numbers affixed reading"27945."

**59.** On January 4, 2023 your affiant observed the residence and observed a subject matching the description of and believed to be Jeremy MILLER exit the residence and enter a vehicle. MILLER departed the area and was observed traveling to a business, DL Martin Machine Company, located at 25 D.L.Martin drive, Mercersburg, PA 17236, where he is believed to be employed.

**60.** HSI Agents programmed ShareazLE to specially ask for downloads from this IP address, 174.54.12.128, for some of the latest files this computer said it had. From those, HSI Agents received thirteen (13) files identified by their Hash value. These files were reviewed by your affiant and confirmed to be CSAM.

**61.** On April 18, 2023 these thirteen (13) hash values were submitted to the National Center for Missing & Exploited Children (NCMEC) for review. Of the thirteen files received, six (6) were of identified children, six (6) of the files were recognized hash values associated

with material previously submitted to NCMEC, and one (1) file was unrecognized, meaning that the hash value has not been submitted to NCMEC previously.

## CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD SEXUAL ABUSE MATERIAL AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

62. Based on my previous investigative experience related to Child Sexual Abuse Material investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple images of Child Sexual Abuse Material are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films,

photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other Child Sexual Abuse Material distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in Child Sexual Abuse Material.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their Child Sexual Abuse Material for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of Child Sexual Abuse Material throughout the world.

g. Based on the repeated offering of Child Sexual Abuse Material for download by others, and his steady building of an apparent collection of Child Sexual Abuse Material over time, the user of the computer at the SUBJECT PREMISES has demonstrated conduct consistent with the behavior of collectors of Child Sexual Abuse Material as discussed above.

## CONCLUSION

63. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. §§ 2252 and 2252A.

64. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B to include a full forensic examination of any computers, electronics, and related devices listed here.

JUSTIN W KURTZ

Digitally signed by JUSTIN W KURTZ
Date: 2023.05.08 12:18:52 -04'00'

Justin Kurtz
Special Agent
Homeland Security Investigations

On this 5th day of May 2023, Justin Kurtz appeared before me, was placed under oath, and attested to the contents of this Affidavit.

s/ Martin C. Carlson
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## DESCRIPTION OF PROPERTY TO BE SEARCHED

The property at 27945 Great Cove Rd, Fort Littleton, PA 17223 is described the residence is described as a single-family manufactured home with blue corrugated metal siding and blue shutters. Attached to the front of the residence is a porch with concrete pad and metal roof with multiple pieces of furniture and a riding lawn mower parked underneath. Attached to the corner of the roof of the porch was a green sign with numbers reading "27945." Located directly in front of the residence is a mailbox with a green sign with numbers affixed reading "27945."

See attached photograph.

# ATTACHMENT B
# PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) evidence of violations of 18 U.S.C. §§ 2252 and 2252A ("subject violations"); or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

1. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, mobile telephone devices, mobile data storage devices, mobile electronic music players, video gaming devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict Child Sexual Abuse Material or child erotica; display or access information pertaining to a sexual interest in Child Sexual Abuse Material; display or access information pertaining to sexual activity with children; or distribute, possess, or receive Child Sexual Abuse Material, child erotica, or information pertaining to an interest in Child Sexual Abuse Material or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of [target's e-mail address] by use of the computer or by other means for the purpose of distributing or receiving Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about Child Sexual Abuse Material or the existence of sites on the Internet that contain Child Sexual Abuse Material or that cater to those with an interest in Child Sexual Abuse Material.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible Child Sexual Abuse Material to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation,

purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any Child Sexual Abuse Material as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

16. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

17. Credit card information, including, but not limited to, bills and payment records.

18. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

19. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.